WHAT IS CLAIMED IS:

1. A method of limiting the amount of time credit card information is valid for use in support of an electronic transaction comprising the following steps:

A. initiating a credit card transaction by accessing a vendor via an internet browser;

B. recording credit card information required by the vendor via the browser;

C obtaining a date/time stamp representing the current time;

D. encrypting said stamp; and

E. transmitting said credit card information and said encrypted stamp to a validating institution for validation, whereby said validating institution may decrypt said encrypted stamp to determine if the age of the proposed transaction as represented by the time of the decrypted stamp is within a predetermined time limit required for validating the transaction.

2. A method according to claim 1 wherein step B includes recording a PIN number as part of the credit card information.

3 A method of limiting the amount of time credit card information is valid for use in support of an electronic transaction comprising the following steps:

A. initiating a credit card transaction by accessing a vendor via an internet browser;

B. recording credit card information required by the vendor via the browser;

C obtaining a date/time stamp representing the current time;

D. using said PIN number and said date/time stamp to generate an ePIN which comprises an encrypted sequence of alphanumeric characters representing said PIN and/or said date/time stamp;

E. transmitting said credit card information and said ePIN to a validating institution for validation, whereby said validating institution may decrypt said ePIN to obtain said date/time stamp and determine if the age of the proposed transaction as represented by the time of the decrypted date/time stamp is within a predetermined time limit required for validating the transaction.

4. A method of conducting electronic credit card transactions so as to guard against fraud, comprising the following steps:

a credit card user initiates a credit card transaction by accessing a credit card validating institution via a third party vendor using an internet browser and transmitting to that validating institution credit card information identifying said user and an encrypted date/time stamp representing the current transaction time obtained from a non-adjustable time source;

said validating institution receives said encrypted date/time stamp and said other credit card information and decrypts said encrypted stamp to derive the current transaction time as represented by said decrypted date/time stamp;

said validating institution (1) compares said credit card information with previously recorded user information to verify that the user initiating the proposed transaction is an authorized user and (2) also compares the current transaction time represented by said decrypted date/time stamp with the time of its receipt of said encrypted date time stamp and determines if the difference, if any, between said times is within a predetermined time limit; and

depending on the determination made in the foregoing step, the validating institution communicates either a validation or rejection of the transaction to the user initiating the proposed transaction.

5. A method according to claim 4 wherein said user also transmits an encrypted PIN to said validating institution, and said validating institution decrypts said PIN as part of its validation process.

6. A method of providing security to an electronic credit card system wherein initiation of a credit card transaction requires the credit card user to transmit specific identifying information to a transaction validating institution, comprising the step of including an encrypted date/time stamp as part of the credit card transaction information that is transmitted to the transaction validating institution, said date/time stamp being derived from a non-adjustable time source and indicating the current time of the proposed transaction, said encrypted date/time stamp being encrypted according to an encryption scheme specified by said transaction validating institution.

7. A method according to claim 6 wherein said transaction information includes a credit card account number and a PIN.

8. A method for providing secure credit card transactions between a first entity and at least one additional entity, comprising the steps of:

(a) establishing a credit card account for the first entity, creating a preset identification code for that account, storing said identification code in a selected validating system, and providing said code to said first entity;

(b) receiving in the validating system for verification a first identification code which is transmitted at the request of a person who may or may not be said first entity, said first identification code being transmitted with other transaction information in connection with a credit card transaction proposed by said person and including an encrypted date/time stamp representing the time that said proposed credit card transaction was initiated by said person;

(c) comparing the time represented by said date/time stamp with the current time provided by a non-adjustable clock; and

(d) rejecting the proposed transaction if there is a difference between the time represented by said date/time stamp and the current time provided by said non-adjustable clock and said difference in time exceeds a predetermined limit.

9. The method of claim 8 further including the step of comparing said first identification code with said pre-set identification code and rejecting the proposed transaction if the first identification code does not conform to said pre-set identification code of said first entity.

10. The method of claim 8 wherein said at least one additional entity is a third party vendor of goods or services, and further wherein said first identification code and said other transaction information are transmitted to said validation system via said third party vendor, said third party vendor having received said first identification code and said other transaction information from said person.

11.. A method for authorizing an electronic business transaction by an authorized user, comprising the steps of:

(a) storing information about authorized users, including pre-set unique identification codes for each authorized user, in a validating system, and providing said identification codes to said authorized users for use in initiating and completing electronic transactions;

(b) receiving in the validating system for verification an identification code which is transmitted in connection with a proposed electronic business transaction at the request of a person who may or may not be an authorized user, said identification code being transmitted and received together with a date/time stamp representing the time that the proposed electronic business transaction was initiated by said person;

(c) comparing said transmitted and received identification code with the pre-set unique identification codes stored in said validating system to verify that it is valid, and rejecting the proposed transaction if said transmitted and received identification code is not valid; and

(d). if said transmitted and received identification code is verified as valid, (a) comparing the time represented by date/time stamp with the time of receipt of said transmitted identification code and date/time stamp by said validating system, and (b)

rejecting the proposed transaction if there is a difference between the time represented by said date/time stamp and said time of receipt, and that difference exceeds a predetermined limit.

12. The method of claim 11 wherein said electronic transactions is a credit card transaction, and each of said unique identification codes include a unique credit card account designation.

13. The method of claim 11 wherein said identification code received by said validating system is transmitted to said validating system via a third party vendor, and further wherein rejection or authorization of said proposed transaction is communicated by said validating system to said vendor.

14. The method of claim 11 wherein said received date/time stamp is encrypted, and further wherein said step (d) is preceded by the step of decrypting said received date/time stamp.

15. The method of claim 11 wherein said received date/time stamp and at least a portion of said received identification code are encrypted, and further wherein step (d) is preceded by a decryption step to decrypt said date/time stamp and the encrypted portion of said received identification code.

16. The method of claim 15 wherein said transmitted and received identification code includes a PIN.

17. The method of claim 16 wherein said PIN in said received identification code is encrypted.

18. The method of claim 11 wherein said transmitted and received identification code includes a PKN.

19. The method of 18 wherein said PKN in said received identification code is encrypted.